AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: /s/ Corbin Houston, 10/13/22

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of)
)
Black iPhone 13 Pro Max with serial number) Case No: MJ-22-752-SM
KXLN60QR4V, stored at HSI)
Oklahoma City Field Office 3625 NW 56th St.)
Oklahoma City, Oklahoma 73112)

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following Property:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed;

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252A	Possession of Child Pornography

The application is based on these facts:

See attached Affidavit of Special Agent Abraham Schenk, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of [No. of Days] days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

ABRAHAM SCHENK
Special Agent
Homeland Security Investigations

Sworn to before me and signed in my presence.

Date: OCT. 14, 2022

Judge's signature

City and State: Oklahoma City, Oklahoma

Suzanne Mitchell, U.S. Magistrate Judge
Printed name and title

THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF OKLAHOMA

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Abraham Schenk, a Special Agent with the Department of Homeland Security, Homeland Security Investigations, being first duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI") since January 2011 and am currently assigned to the Office of the Resident Agent in Charge, Oklahoma City, Oklahoma. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime and have gained experience investigating federal child exploitation and child pornography violations through training at the Federal Law Enforcement Training Center and the Internet Crimes Against Children (ICAC) Task Force, Oklahoma City, working with other more experienced child exploitation criminal investigators, and learning from my own child exploitation investigations, which I have been conducting since 2017.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I am investigating the online activities of Braeden WOOD, who is alleged to have possessed child pornography, in violation of 18 U.S.C. § 2252A (the "SUBJECT OFFENSE").

4. This Affidavit seeks authorization to search a Black iPhone 13 Pro Max, further described in Attachment A and referred to as the "SUBJECT DEVICE," and seize

therefrom the items described in Attachment B, which constitute instrumentalities, fruits, and evidence of the SUBJECT OFFENSE.

5. I seized the SUBJECT DEVICE from WOOD's person on October 13, 2022, following the execution of a federal search warrant related to the investigation into WOOD. As set forth below, there is probable cause to believe that WOOD possessed, owned, and used the SUBJECT DEVICE to commit the SUBJECT OFFENSE.

6. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

7. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on devices. This information can sometimes be recovered with forensics tools.

8. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities. These photos are sometimes stored in cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may contain notes

regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or more persons to communicate information regarding illegal activities.

9. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications, as well as applications like Snapchat. Additionally, individuals utilize their cellular devices to take and store pictures and keep notes. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual.

10. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during, and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, and phone call histories.

11. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the SUBJECT OFFENSE, but also forensic evidence that establishes how the SUBJECT DEVICE was used, the purpose of its use, who used it, and when. There

is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

12. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICE consistent with the warrant. The examination may require authorities to employ techniques (including but not limited to computer-assisted scans of the entire medium) that might expose many parts of the SUBJECT DEVICE to human inspection in order to determine whether it is evidence described by the warrant.

13. *Manner of execution.* Because this warrant seeks only permission to examine the SUBJECT DEVICE already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, there is reasonable cause to authorize execution of the warrant at any time in the day or night.

14. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime under investigation, including but not limited to undertaking a cursory inspection of all information within the SUBJECT DEVICE. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon

to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

STATEMENT OF PROBABLE CAUSE

15. In March 2022, HSI Oklahoma City received Cybertip 109513299 from the National Center for Missing and Exploited Children (NCMEC), which had been reported by the electronic service provider Synchronoss Technologies, Inc.[1] Cybertip 109513299 indicated a Verizon Cloud account user with associated phone number 405-802-6802 had uploaded approximately 52 image files containing child pornography to his/her Verizon Cloud account ("SUSPECT ACCOUNT") on or about December 2, 2021.

16. On March 7, 2022, I reviewed the 52 image files and verified that at least 31 of the images met the federal definition of child pornography. The following are two representative examples of the images I observed from the 31 images designation as child pornography:

(a) Filename: 078894ef2e78425f8a97729874276e60_file51

Hash Value (MD5): 80e97fa434e08bf50f761ef5e360e19b

Observation: A color image of a prepubescent female laying on her back (nude from the chest down – only wearing a pajama top) with her legs spread open and her vaginal area fully exposed.

(b) Filename: 078894ef2e78425f8a97729874276e60_file17

[1] Synchronoss Technologies Inc. is the cloud-based storage provider for the digital content stored on a Verizon user's Verizon Cloud account.

Hash Value (MD5): 366f282e13b10adfbd7e7154b55af04a

Observation: A color image of a prepubescent female vagina (close-up); the exterior of the vagina being spread open by the fingers of an adult hand.

17. On March 8, 2022, I served a summons to Verizon Wireless for the subscriber information associated with phone number 405-802-6802 covering the time period of December 2, 2021. On March 10, 2021, Verizon responded with the following account holder information:

- Account Number: 426006882-1
- Subscriber Name: Braedon Wood (herein "WOOD")
- Account Effective Date: 09/03/2020
- Subscriber Address: 1400 E Main St, Moore, OK 73160-7845
- Device Type: Samsung Note 20 5G Mint 128GB
- Device IMEI: 350680830145665
- Device IMSI: 311480598741831

18. Additionally, Verizon provided a spreadsheet listing the account features included in the SUSPECT ACCOUNT and their respective activation/deactivation dates. Among those features included was 600gb Verizon Cloud storage, which was active on December 4, 2020, and no associated deactivation date. A review of the LexisNexis Accurint law enforcement database revealed WOOD had a listed address of 1400 E Main Street, Moore, Oklahoma, in November 2020. The database listed his most recent address as 18130 E. Tecumseh Road, Newalla, Oklahoma 74857 (i.e., the SUBJECT PREMISES).

19. On March 15, 2022, HSI Oklahoma City received another Cybertip (117158858) from NCMEC via Synchronoss Technologies, Inc., indicating that the SUSPECT ACCOUNT had

again uploaded approximately 72 image files containing child pornography on February 1, 2022. I reviewed the 72 image files and verified that at least 31 of the images met the federal definition of child pornography. The following are two representative examples of the images I observed from the 31 images designated as child pornography:

(a) Filename:

078894ef2e78425f8a97729874276e60_6fca9f02cb5e57cedf9d00b2df53122e43479fc9a8e8e4e7b968e82247d1e0dc.zip

Hash Value (MD5): bb06a0745021d2406cb45b300d7b8bdc

Observation: A color image of a prepubescent female toddler laying on her back fully nude with her legs spread open while an adult male hand spreads open her vagina.

(b) Filename:

078894ef2e78425f8a97729874276e60_134b20a036f425f87c30ebf86be447cb8fae5fce81ca1b4a7657112860009654.zip

Hash Value (MD5): 48f05d37fef6a5d2e8ce8bf4a80a2c30

Observation: A color image of a prepubescent female laying on her back with her legs spread open (vagina fully exposed) and a pink object inserted inside her vagina.

20. In April 2022, I conducted a search of Facebook.com and discovered two Facebook accounts under the name of "Braedon Wood" (facebook.com/Braedon.wood.5 and facebook.com/profile.php?id=100080025115060; both with photographs of WOOD). During my review of both accounts, I observed profile photos in each account that showed a black Dodge Charger parked in front of a house matching the SUBJECT PREMISES. Additionally, in one of

the Facebook accounts I observed a memorandum to "Braedon Wood" from the Air Force Materiel Command requiring all Department of Defense (DOD) employees to receive the Coronavirus vaccination. On May 5, 2022, I requested verification of federal employment from Air Force Office of Special Investigations (AFOSI) Special Agent (SA) Charles Woford, who queried the DOD employee database and returned a screenshot confirming WOOD was a DOD employee and worked at Tinker Air Force Base.

21. On May 12, 2022, I applied for and was granted a federal search warrant in the Western District of Oklahoma for the contents of the SUSPECT ACCOUNT. On May 18, 2022, I served the search warrant on Synchronoss Technologies, Inc. via email and received the returned contents on May 25, 2022. I thereafter reviewed the contents of the SUSPECT ACCOUNT and observed the following:

- A short color video of a pre-pubescent girl sitting on a toilet with her genitals exposed. The video appeared to be recorded using a cell phone and a man's foot and bathrobe can be seen from the view of the person recording the video;
- Several photographs of WOOD's room, which appears to be a converted garage, complete with bed, couch, dining room table, kitchen and TV;
- Several images of post-pubescent girls wearing diapers;
- A screenshot showing a home address as 1400 E. Main Street, Moore, OK 73160 on March 23, 2022;
- A screenshot that shows the definition of DDLG (Daddy Dom Little Girl) – a term known to be associated with an adult male sexually interested in young girls and vice versa;

- Several images of a black Dodge Charger with the license plate OK/HTB145;
- Several photographs of WOOD with the Dodge Charger in the driveway of a house that matches the house, driveway and brick wall (alongside the driveway) of the SUBJECT PREMISES. The house is completely brick, except for the section in front of the driveway, which appears to have vinyl siding – consistent with a garage that has been remodeled and converted into a bedroom;
- Several images of WOOD lying in bed with his girlfriend, who has a pacifier in her mouth;
- A video of an adult male wearing only a diaper full of urine. Based on the filename convention and the shape/size of the legs and torse, the male appears to be WOOD. There are also several images of the adult male wearing the diaper, holding it up and showing it open (filled with urine).

Additionally, I observed 72 videos and 2 images that met the federal definition of child pornography. The following are two representative examples of the videos I observed from the 72 videos designated as child pornography:

(a) Filename: VID-20171114-WA0071.mp4

Hash Value (MD5): 63942F05CC55CE517F255898B20D3FB1

Observation: A color video lasting approximately 20 seconds showing an adult female wearing only underwear holding a nude male infant over her head while performing oral sex on the infant's penis.

(b) Filename: [PTHC] 5yo Gets The Complete Treatment.rm

Hash Value (MD5): ED38A2BA07B8E04A606A2CEE4B62A3A5

Observation: A color video lasting approximately 11 minutes showing an adult male penetrating the exposed vagina of a prepubescent female with his penis in various positions, then forcing her to perform oral sex on him. After engaging in additional sexual intercourse with the prepubescent female, the adult male ejaculated on her face.

22. Between July 14 and July 28, 2022, I conducted surveillance at the SUBJECT PREMISES and each time observed a black Dodge Charger matching the photos in the SUSPECT ACCOUNT, but each time the vehicle was parked with its back to the house, so the license plate was not visible.

23. On August 1, 2022, AFOSI SA Woford sent me a new screenshot from a database query of the DOD employee database indicating WOOD had recently updated his home and mailing address to 18130 E. Tecumseh Road, Newalla, OK 74857.[2]

24. On September 9, 2022, I again conducted surveillance at the SUBJECT PREMISES and observed the Dodge Charger in the driveway at approximately 7:10 A.M. At approximately 7:15 A.M., the Dodge Charger was no longer there. I then drove to Tinker Air Force Base, building 9001 (where WOOD was known to be employed), and observed the black Dodge Charger with Oklahoma license plate number HTB145 parked in the parking lot of building 9001 at approximately 8:08 A.M.. The Dodge Charger had two car seats in the back seat. Later that day, at approximately 3:56 P.M., I observed WOOD exit building 9001 and leave the base driving the Dodge Charger. At approximately 4:07 P.M., I observed WOOD pull into the New Life Baptist

[2] On May 5, 2022, AFOSI SA Woford queried the DOD employee database to verify that WOOD was an Air Force civilian employee. During that database query, WOOD's listed address was 10317 SE 44th Street, Oklahoma City, OK 73150. The database query also revealed WOOD worked at Tinker Air Force Base in Building 9001.

Church parking lot (which operates a daycare) on Peebly Road (which is on the way to Tecumseh Road). At approximately 4:19 P.M., I observed WOOD pull into Lett Circle from 149th Street (all in the vicinity of the SUBJECT PREMISES), which is a private drive. Unable to follow WOOD down the private drive, I returned to the area of the SUBJECT PREMISES. At approximately 4:47 P.M., I observed the Dodge Charger turn into Tecumseh Road and enter the driveway to the SUBJECT PREMISES. Before parking, the Dodge Charger again pulled out of the SUBJECT PREMISES and headed south on Dobbs Road. At approximately 4:53 P.M., I observed WOOD in the driver's seat of the Dodge Charger (his window was rolled down) in the drive-thru line at the Sonic on the corner of S Dobbs Road and E Robinson Road.

SEARCH WARRANT EXECUTION

25. On October 7, 2022, I applied for and obtained a federal search warrant for the SUBJECT PREMISES. On October 13, 2022, at approximately 6:30 A.M., HSI Oklahoma City executed the warrant at the SUBJECT PREMISES. WOOD was not encountered at the location. Given the exigent circumstances, Special Agent Rachel Cathie and I located WOOD at his place of employment on Tinker Air Force Base in Midwest City, Oklahoma. After I read a *Miranda* warning to WOOD, WOOD agreed to speak to agents without the presence of an attorney. During his interview, WOOD stated he has possessed the phone number 405-802-6802 since 2007. WOOD also stated that the Samsung G20 Note cell phone identified by the investigation is in fact his previous cell phone. He purchased a new phone, an Apple iPhone 13, in April of 2022. Wood admitted to downloading and viewing child pornography on his Samsung cell phone coinciding with the dates of the two NCMEC cybertips discussed herein. WOOD also admitted to viewing child pornography a "couple of days ago," by accessing a website that hosts child pornography on his current iPhone 13 while he was at work, in a government facility. When

asked how he accessed the website with child pornography, WOOD brought up the internet history on his cell phone (the iPhone 13) and showed me the website.

26. Following the interview, I detained WOOD's current cell phone and further identified it as a black Apple iPhone 13 Pro Max, serial number KXLN60QR4V

27. Based upon the foregoing, I believe there is probable cause that WOOD violated 18 U.S.C. § 2252A. Therefore, I respectfully request that a warrant be issued for his arrest.

CONCLUSION

28. Based on the foregoing, there is probable cause to believe that the SUBJECT OFFENSE has been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located on the SUBJECT DEVICE. I respectfully request that this Court issue a search warrant authorizing the search of the SUBJECT DEVICE described in Attachment A to seize the items described in Attachment B.

Abraham Schenk
Special Agent
Homeland Security Investigations

SUBSCRIBED AND SWORN to before me this 14th day of October, 2022.

SUZANNE MITCHELL
United States Magistrate Judge

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant seeks to search a Black iPhone 13 Pro Max with serial number KXLN60QR4V. The SUBJECT DEVICE is currently located at the HSI Oklahoma City Field Office, located at 3625 NW 56th Street, Oklahoma City, Oklahoma 73112.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. All records on the SUBJECT DEVICE described in Attachment A that relate to violations of the SUBJECT OFFENSE:

I. Digital Evidence

1. Any passwords, password files, test keys, encryption codes, or other information necessary to access the SUBJECT DEVICE;

2. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device described in Attachment A, that show the actual user(s) of the computer or digital device during the time the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the device; MAC IDs and/or Internet Protocol addresses used by the device; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software; evidence of the absence of such malicious software, or of the presence or absence of security software designed to detect malicious software;

3. Evidence that the device was attached to or used as a data storage device for some other device, or that another device was attached to the device; and

4. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer or digital device;

II. Records, Documents, and Visual Depictions

1. Any records, documents, or materials, including correspondence, that pertain to any conversations with the UCA described in the Affidavit in support of the search warrant application in any form including Kik, or any other social media platform;

2. Any records, documents, or materials, including any correspondence, that involve any communication with any person that appear to be coercive in nature for the purposes of grooming or obtaining images from any person;

3. Any records, documents, or materials, including correspondence, that pertain to the production, transportation, distribution, receipt, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

4. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

5. Any motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

6. Any records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

7. Any records, documents, or materials relating to the production, reproduction, receipt, shipment, trade, purchase, or a transaction of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

8. Any records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

9. Any records of Internet usage, including records containing screen names, usernames, and e-mail addresses, and identities assumed for the purposes of communication on the Internet on any app installed on the SUBJECT DEVICE.

10. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of distributing or transporting child pornography, including chat logs, call logs, address book or contact list entries, digital images sent or received;

11. Information or evidence of any websites visited, photographs, videos, images, reports, definitions, stories, books, music, lyrics, emails, videos, messages, and or

notes associated with child pornography or those who collect, disseminate, or trade in child pornography; and

12. Any records, documents, materials, videos, or photographs that would allow investigators to ascertain who used the SUBJECT DEVICE;

As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified or stored in any form including digital or electronic form.